

**AFFIDAVIT IN SUPPORT OF  
APPLICATION FOR A SEARCH WARRANT**

I, Derek Judd, being duly sworn, depose and say:

Introduction

1. I am a Special Agent with Homeland Security Investigations (HSI), presently assigned to HSI's Derby Line, Vermont office. HSI is a directorate within Immigration and Customs Enforcement (ICE). ICE is a component of the Department of Homeland Security (DHS) and the successor to many of the law enforcement powers of the former Immigration and Naturalization Service and U.S. Customs Service. I have been a Special Agent since March 2008, and graduated from the Federal Law Enforcement Training Center in July 2008. I hold a Bachelor of Arts degree in Social Science from Lyndon State College and a Master of Science degree in Criminal Justice from the University of Cincinnati.

2. My duties as an HSI Special Agent include investigating violations of Titles 18 and 21 of the United States Code, including offenses relating to the importation, possession, and distribution of controlled substances. In the course of my law enforcement career, I have executed search and arrest warrants, interviewed subjects, witnesses, and victims, and conducted surveillance. I have also gained an understanding of current technology through my work as an HSI Special Agent, including knowledge regarding computers and online accounts, cellular telephones and smart phones, and associated records and data; and I have conducted analyses of data related to such accounts and devices.

3. I am submitting this Affidavit in support of an Application for a Search Warrant authorizing the search of an Apple iPhone more specifically described below and in Attachment A (the "Target Device"). As set forth below, the Target Device is associated with Yensi J. ROSA-TAVERAS. There is probable cause to believe that ROSA-TAVERAS and others have violated

21 U.S.C. §§ 841(a) and 846 through the possession with intent to distribute and/or conspiracy to distribute controlled substances, among other offenses. There is also probable cause to believe that ROSA-TAVERAS has violated 18 U.S.C. § 922(g)(3) by possessing a firearm while a user of or addicted to a controlled substance. There is further probable cause to believe that the information described in Attachment B will provide evidence of those crimes.

4. I have been investigating these crimes since January 2021 and have reviewed materials including data obtained by the Vermont State Police (VSP) pursuant to a state search warrant for the Target Device. I seek this warrant in an abundance of caution to authorize forensic analysis of the Target Device and additional review of data from the Target Device using different forensic tools, and to search the Target Device for evidence of federal offenses beyond the scope of the state warrant. Since this affidavit is being submitted for the limited purpose of supporting a search warrant application, I have not included all the details I know regarding every aspect of the investigation. Except as otherwise noted, the information contained in this affidavit is based upon my personal knowledge and observations, my training and experience, conversations with other law enforcement officers and witnesses, and my review of documents and records.

#### Probable Cause

5. VSP Detective Trooper Andrew Todd summarized some of the pertinent facts relating to this investigation in his affidavit dated February 5, 2021 (the "Todd Affidavit"). The Todd Affidavit is attached as Exhibit 1 and incorporated herein by reference.

6. As set forth in the Todd Affidavit, this investigation concerns a package from the Dominican Republic that arrived in the United States bound for Vermont on or about January 22, 2021. U.S. Customs and Border Protection Officers inspected the package at the Hernandez Airport in Puerto Rico; a drug-detection K-9 alerted to the odor of narcotics in the package, and

an x-ray scan of the package revealed abnormalities within the cardboard layers of its packaging. A search of the package yielded over 200 grams of cocaine.

7. The package was addressed to “Josefina Velazquez” at 52 Erad Apt #4 in Sharon, Vermont. As the Todd Affidavit describes, the recipient’s name appeared to be fictitious.

8. On January 28, 2021, I conducted a controlled delivery of the package. Miranda Potter accepted the package in the parking lot outside the apartment building and took it inside Apartment 4. Members of law enforcement then executed an anticipatory search warrant.

9. Among other things, the search of the apartment and its basement pursuant to that warrant yielded marijuana plants and firearms including a Ruger pistol, a Savage Axis rifle, and ammunition. Investigators also found a digital scale inside the apartment. Field testing of residue on the scale yielded a positive result for the presence of cocaine.

10. Members of law enforcement found the Target Device in Apartment 4’s master bedroom, on a stand next to the bed. ROSA-TAVERAS and Potter indicated that the Target Device belonged to ROSA-TAVERAS. ROSA-TAVERAS declined to consent to a search of the Target Device, which was then seized pending issuance of a Vermont state search warrant.

11. ROSA-TAVERAS and Potter were both present inside Apartment 4 when the anticipatory search warrant was executed. Potter waived her *Miranda* rights and spoke with law enforcement on scene. Among other things, Potter said that she was ROSA-TAVERAS’s girlfriend and that ROSA-TAVERAS lived in the apartment. Potter further indicated that ROSA-TAVERAS was from the Dominican Republic. She said that she had been expecting a delivery of marijuana seeds, but insisted that she did not know there was cocaine in the package she accepted from me during the controlled delivery referenced above. Potter also said that ROSA-TAVERAS had ordered the marijuana seeds she was expecting using his phone (i.e., the Target Device).

12. ROSA-TAVERAS also waived his *Miranda* rights and agreed to speak with law enforcement on scene. Among other things, ROSA-TAVERAS said that he lived in Apartment 4 and that he had been expecting a package with marijuana seeds. He further confirmed that he was from the Dominican Republic and kept in touch with relatives there. He admitted to growing and using marijuana. However, ROSA-TAVERAS denied knowing that the package Miranda Potter accepted from me via the controlled delivery contained cocaine. ROSA-TAVERAS acknowledged that he used the Target Device to access the Internet, but denied using the Target Device to order marijuana seeds. ROSA-TAVERAS further said that he had not purchased the firearms found in the apartment. However, he admitted that he had shot the rifle.

13. A Vermont state search warrant for the Target Device was executed on February 23, 2021. A copy of the Search Warrant Inventory and Return for that warrant is attached as Exhibit 2. As noted above, I reviewed some of the data extracted from the Target Device pursuant to the state warrant, including saved messages. Based on my training and experience, certain of these messages appear to be coded communications consistent with drug trafficking.

14. I am also informed that investigators analyzed the Target Device pursuant to the state warrant and learned the Target Device bore the serial number C39ZN3H0N6XR and was associated with the call number 802-291-2970 and IMEI numbers 353233103666228, 356647082916527, and 353233103585097. Though investigators analyzing the device pursuant to the state warrant successfully extracted some data from the Target Device by means of a “GrayKey” device, the data was extracted in an unindexed format incompatible with certain data review platforms. Based on my training and experience, and my conversations with other members of HSI with digital forensics experience, I believe that a fresh extraction of the data from

the Target Device using tools available to HSI will yield a complete and indexed set of data amenable to further analysis and forensic review.

15. Accordingly, based on the information set forth above and in the Todd Affidavit, there is probable cause to believe that evidence of violations of 21 U.S.C. §§ 841(a) and 846 (possession with intent to distribute and conspiracy to distribute controlled substances) and 18 U.S.C. § 922(g)(3) (possession of a firearm by a user or person addicted to a controlled substance) (together, the “Subject Offenses”) will be found on the Target Device, and that an HSI forensic extraction of the data on the Target Device will yield such evidence in a format reviewable by investigators assigned to this case.

#### Definitions

16. The following non-exhaustive list of definitions applies to this Affidavit and its Attachments:

a. “Digital device” includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips; and security devices. Digital device also includes computers, as defined pursuant to 18 U.S.C. § 1030(e)(1) to mean “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

b. “Computer hardware” consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, mobile telephones, video gaming devices, portable electronic music players, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. “Wireless telephone” (or mobile telephone, or cellular telephone, or iPhone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

d. “Computer software” is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. “Computer passwords, pass-phrases, and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “Internet Service Providers” (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “email address,” an email mailbox, and a personal password selected by the subscriber.

h. “ISP Records” are records maintained by ISPs pertaining to their subscribers, and may include account application information, subscriber and billing information, account access

information (often in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISPs' servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data.

i. "Internet Protocol address" or "IP address" refers to an identifier used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP often assigns a different IP address to a subscriber's modem when it accesses the Internet. IP addresses might also be static, that is, an ISP assigns a subscriber's modem a particular IP address that does not change.

j. "Electronic communications system" refers to any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for electronic storage of such communications.

k. "Electronic Communications Service Providers" (ECSPs) are commercial organizations which provide individuals and businesses the ability to send or receive wire or electronic communications.

l. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies, pictures), mechanical form (including, but not limited to, phonograph records, printing, typing) or electronic or magnetic form (including, but not limited to, tape recordings, storage devices such as flash storage devices [such as SD cards, compact flash, USB flash drives, etc.], floppy disks, hard drives, CD-ROMs, digital video disks (DVDs), PDAs, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device). These terms also include any applications (e.g. software programs). The term "communications" expressly includes, among other things, emails, instant messages, chat logs, correspondence attached to emails (or drafts).

m. "Imaging" or "copying" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents but attributes may change during the reproduction.

n. "Hash value," or "SHA-1," refers to a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data. Secure Hash Algorithm Version 1, or SHA-1, is a mathematical algorithm. SHA-1 was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA). The United States of America has adopted the SHA-1 hash

algorithm described herein as a Federal Information Processing Standard. It is computationally infeasible ( $2^{160}$ ) to find two different files that produce the same SHA-1 value. This allows investigators to identify a file by the value, regardless of the name of the file beyond 99.99 percent certainty. The SHA-1 digital signature can be explained as a digital fingerprint, or DNA of the file.

### Background Regarding Digital Devices

17. Based upon my training and experience, and my discussions with other law enforcement officials, I know the following:

a. Users of digital devices increasingly choose to store items in digital form (e.g. pictures or documents) because digital data takes up less physical space, and can be easily organized and searched. Users also choose to store data in their digital devices because it is more convenient for them to access data in devices they own, rather than to later spend time searching for it. Keeping things in digital form can be safer because data can be easily copied and stored off site as a failsafe.

b. Users also increasingly store things in digital form because storage continues to become less expensive. Today, one terabyte (TB) hard drives are not uncommon in computers. As a rule of thumb, users with one gigabyte of storage space can store the equivalent of 500,000 double spaced pages of text. Thus, each computer can easily contain the equivalent of 500 million pages, that, if printed, would fill six 35' x 35' x 10' rooms. Similarly, a one TB drive could contain 900 full run movies, or 900,000 songs, or four million images. With digital devices, users can store data for years at little cost to no cost.

c. Storing data in digital form and not deleting it mirrors users' online habits where users have, for many years, been encouraged to never delete their emails. For example, since June 2007, Google, Inc. has promoted free, increasingly larger storage "so you should never have to delete mail." See Bill Kee, *Welcome to Official Gmail Blog*, <https://gmail.googleblog.com/2007/06/welcome-to-official-gmail-blog.html> (July 3, 2007); see also Rob Siembroski, *More Gmail Storage Coming For All*, <https://gmail.googleblog.com/2007/10/more-gmail-storage-coming-for-all.html> (Oct. 12, 2007) (promoting its "Infinity+1" plan to constantly give subscribers more storage).

d. Digital devices can also store data automatically, without a user's input. For example, network logs may track an employee's actions for company auditing purposes or email headers may automatically list the servers which transmitted the email. Similarly, a web browser (i.e. an application such as Internet Explorer used to access web pages) can track a user's history of websites visited so users can more easily re-access those sites. Browsers also temporarily cache files from recently accessed web pages to improve the user's experience by reducing that page's loading time. These examples illustrate how the interaction between software and operating systems often results in data being stored without a user's knowledge. Even if a sophisticated user understands this automatic storage of data, attempts at deleting this data often fail because the data may be automatically stored multiple times and in different locations. Thus, digital evidence may exist despite attempts at deleting it.

a. Digital data is practically resilient to deletion. First, as noted, data is often automatically stored multiple times in multiple locations, where even sophisticated users may not be able to locate. Second, digital data can be recovered years after it has been saved, or viewed even after such data has been deleted. For example, when a user deletes a file on a computer, the file is sent to the recycle bin, where it can still be retrieved. Even if the file is deleted from the recycle bin, the data does not actually disappear; rather it remains in “free space” or “slack space” (i.e. in unused space) until it is overwritten by new data. Third, an operating system may also keep deleted data in a “recovery” or “swap file.” Fourth, files from websites are automatically retained in a temporary cache which is only overwritten as they are replaced with more recently viewed web pages. Thus, the ability to retrieve residues of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer use habits.

#### Specifics of Searches and Seizures of Digital Devices

18. Based on my training, my experience, and information provided to me by those involved in the forensic examination of digital devices including cell phones, I know that completely segregating information before an examiner has started reviewing digital evidence is inconsistent with the evidence assessment process. This is true for the following reasons:

a. This application seeks permission to locate and seize not only data that might serve as direct evidence of the Subject Offenses, but also for evidence that establishes how digital devices were used, the purpose of their use, and who used them. Additionally, this application seeks information about the possible location of other evidence.

b. This application seeks permission to search and seize evidence, fruits, or instrumentalities found in the devices described in Attachment A. Some of these items may be files and other data that is generated by a user (e.g. documents, pictures, and videos). Alternatively, other items may be device generated data that becomes meaningful only upon forensic analysis. For example, as noted, a hard drive may contain records of how a computer was used, the purposes for which it was used, and who has used these records. These items are the subject of this warrant.

c. For instance, based upon my training, my experience, and information provided by others involved in the forensic examination of digital devices, I know the following: First, as noted, data that is not currently associated with any file can provide evidence of a file that once existed, but which has since been deleted or altered. This can include a deleted portion of a file (e.g. a paragraph deleted from a document). Second, applications such as web browsers, email, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Third, operating systems can record information, such as the attachment of peripherals (e.g. USB flash drives), and the times the device was in use. Similarly, file systems record the dates files were created and the sequence in which they were created. Any of this

information may be evidence of a crime, or indicate the existence and location of evidence in other locations on the digital device.

d. In determining how a digital device has been used, the purpose for which it was used, and who has used it, it is sometimes necessary to establish that a particular thing is not present. For example, in cases where more than one person has used a digital device, agents can infer that a defendant must have been the person who used that device to commit a crime by eliminating the possibility that other people used that device during that time. Because file systems often list the dates and times those files were created, this information can help exclude the possibility that other people were using that digital device. As another example, by reviewing a computer's Index.dat files (a system file that keeps track of activity conducted in Internet Explorer), a forensic examiner can determine whether a user accessed other information close in time to the file creation dates, times, and sequences so as to establish user identity and exclude others as having used that computer during times related to the criminal activity. Demonstrating the significance of the absence of certain data on a digital device may require analysis of the digital device as a whole.

e. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a user or excluding a user. All of these types of evidence may indicate ownership, knowledge, and intent.

b. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

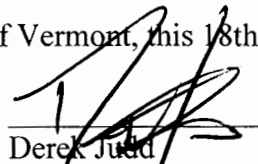
19. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all texts or emails stored on the Target Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data

as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account or stored on a device, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account or stored on a device that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

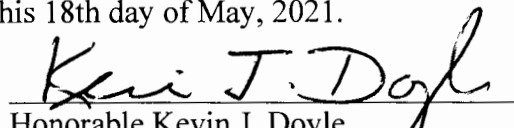
20. Based on my training, my experience, and information given to me by others involved in the forensic examination of digital devices, I know that searching for this kind of evidence involves technical, complex, and dynamic processes, which may require expertise, specialized equipment and a knowledge of how digital devices are often used to commit the Subject Offenses.

21. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of these warrants does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrants at any time in the day or night.

Dated at Burlington, in the District of Vermont, this 18th day of May, 2021.

  
Derek Judd  
Special Agent, HSI

Sworn to and subscribed before me this 18th day of May, 2021.

  
Honorable Kevin J. Doyle  
United States Magistrate Judge